

August 30, 2018

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

**Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity,
FERC Docket No. NP18-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty¹ regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).²

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violation,³ with the Commission because the Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of a violation of NERC Critical Infrastructure Protection (CIP) Reliability Standards.

¹ *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). See also 18 C.F.R. Part 39 (2018). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). See 18 C.F.R § 39.7(c)(2).

² See 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

³ For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC Notice of Penalty
Unidentified Registered Entity
August 30, 2018
Page 2

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

According to the Settlement Agreement, URE admits to the violation and has agreed to actions to mitigate the instant violation and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violation

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission’s regulations, 18 C.F.R. § 39.7 (2018), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method						
*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation						
NERC Violation ID	Standard	Req.	VRF/VSL	Discovery Method*	Risk	Penalty Amount
WECC2015015218	CIP-005-3a	R1	Medium/ Severe	CA	Serious	No Penalty

WECC2015015218 CIP-005-3a R1 - OVERVIEW

During a Compliance Audit, WECC reviewed URE's network diagrams and determined that URE was in noncompliance with CIP-005-3a R1. Specifically, WECC discovered that URE failed to accurately identify and document all electronic access points to the Electronic Security Perimeters (ESPs) as required in CIP-005-3a R1. URE used layer 2 switches to segment ESP networks from untrusted non-ESP virtual local area networks (VLANs), creating a mixed-trust environment with possible access to Critical Cyber Assets (CCAs) within the ESP. This mixed-trust environment established external routable connectivity into the ESP without going through an identified Electronic Access Point, contrary to the CIP requirement. WECC was not able to verify the security controls associated with the non-CIP VLANs.

The root cause of this noncompliance was a misinterpretation of the Standard. URE did not consider the layer 2 switches on the non-ESP VLANs as access points to the ESP.

NERC Notice of Penalty
Unidentified Registered Entity
August 30, 2018
Page 3

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

WECC determined that this violation posed a serious risk to the reliability and security of the bulk power system (BPS). In this instance, URE failed to identify and document access points to the ESP as required by CIP-005-3a R1. Specifically, URE utilized layer 2 switches to logically segment ESP networks from untrusted non-ESP VLANs at multiple facilities. Not properly verifying access permissions into the ESP increased the likelihood of an unauthorized user gaining access to URE facilities. This could have potentially resulted in an unauthorized user gaining access to a non-CIP environment and “hopping” VLANs to gain access to CCAs inside the ESP. This could have led to the misoperation of Bulk Electric System (BES) elements.

URE did not have any controls in place to ensure an unauthorized user did not have access to the layer 2 devices from a non-CIP VLAN and gain access to CCAs inside the ESP. Additionally, URE did not have appropriate controls in place to identify when an unauthorized user attempted to gain, or successfully gained, access to ESP assets.

WECC could not confirm the protections or security controls that the logical segmentation on URE’s layer 2 switches provided to the CCAs inside the ESPs. NERC’s approach to an ESP trusted enclave identified in CIP-005-3 R1 includes the definition of an ESP (the logical border surrounding a network to which BES Cyber Systems are connected) that requires the security controls identified in the CIP Standards, which is a network (layer 3) security control. A layer 2 switch cannot provide these security controls.

WECC determined the duration of the violation to be approximately six and one-half years, from the date the Standard became mandatory and enforceable, through when URE removed the layer 2 switches and access for the non-CIP VLANs was revoked.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. developed a new supervisory control and data acquisition (SCADA) and operations network design that removes all mixed-trust layer 2 switches;
2. reviewed and received approval on the new design from the SCADA and Compliance departments; and
3. implemented the new design to remove all mixed-trust environment layer 2 switches.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

NERC Notice of Penalty
Unidentified Registered Entity
August 30, 2018
Page 4

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Regional Entity's Basis for Penalty

WECC proposed no monetary penalty for the violation. In reaching this determination, WECC considered the following factors:

1. WECC determined URE's compliance history should not serve as an aggravating factor;
2. WECC did not provide mitigating credit for URE's internal compliance program. URE did not have any detective controls in place that could have helped identify the issues sooner to lessen the violation duration and thereby lessen the risk;
3. URE admitted to the violation;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt by URE to conceal the violation nor evidence of intent to do so;
6. the violation posed a serious risk to the reliability and security of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed would-be penalty.

After consideration of the above factors, WECC determined that, in this instance, no financial penalty is appropriate.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed⁴

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,⁵ the NERC BOTCC reviewed the violation on August 14, 2018, and approved the terms of the Settlement Agreement. In approving the resolution, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violation at issue.

⁴ See 18 C.F.R. § 39.7(d)(4).

⁵ *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

NERC Notice of Penalty
Unidentified Registered Entity
August 30, 2018
Page 5

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

For the foregoing reasons, the NERC BOTCC approved the terms of the Settlement Agreement and believes that the proposed resolution is appropriate for the violation and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability and security of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the Notice of Penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the Notice of Penalty, upon final determination by FERC.

NERC Notice of Penalty
Unidentified Registered Entity
August 30, 2018
Page 6

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

<p>Melanie Frye* President and Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6882 (801) 883-6894 – facsimile mfrye@wecc.biz</p> <p>Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile raredondo@wecc.biz</p> <p>Heather Laws* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz</p>	<p>Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net</p> <p>Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net</p> <p>Emily Burgis* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile emily.burgis@nerc.net</p>
---	---

NERC Notice of Penalty
Unidentified Registered Entity
August 30, 2018
Page 7

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Emily Burgis

Sonia C. Mendonça
Vice President, Deputy General Counsel,
and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of
Enforcement Oversight
Emily Burgis
Associate Counsel
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
emily.burgis@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council